UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,392	07/26/2001	Alex James Hinchliffe	01.054.01	5032

7590 08/04/2006

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/912,392	HINCHLIFFE ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *7-27,34-54 and 61-81* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *7-27,34-54 and 61-81* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 4/7/2005.

DETAILED ACTION

Response to Arguments

The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

However, as the examiner had previously, and improperly, suggested that the claims be renumbered, and in order to expedite prosecution of this application, the examiner has allowed the renumbered claims to be entered. However, as there are now two claims numbered 34, and two numbered 61, and no claims 28, or 55, the examiner has provided the following correction.

Original claims 29-34, and 56-61 have been renumbered to 28-33, and 55-60 respectively. As such, claims 7-27, 34-54, and 61-81 are pending and claims 1-6, 28-33, and 55-60, and 82 have been cancelled.

Applicant's arguments with respect to the previously applied prior art have been considered but are moot in view of the new ground(s) of rejection.

Claims 7-27, 34-54, and 61-81 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7-13, 16-24, 27, 34-40, 43-51, 54, 61-67, 70-78, and 81 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hruska et al. (US Patent Number 6,195,587) hereinafter referred to as Hruska, and further in view of Le Pennec et al. (US Patent Number 6,892,303) hereinafter referred to as Le Pennec.

Regarding claims 7, and 17, Hruska disclosed a computer program product for controlling a computer to detect malware, said computer program product comprising (See Hruska Abstract and Col. 3 Lines 40-54 where it was implied that a computer program product was implemented in this system because the system relies on processors, which rely on computer programs): file access request detecting logic operable to detect a file access request to a computer file by a requesting computer (See Hruska Col. 3 lines 63-65); file access clearance request generating logic operable to generate a file access clearance request including data identifying said computer file (See Hruska Col. 3 Lines 20-24 and Col. 4 Lines 20-23); file access clearance request transmitting logic operable to transmit said file access clearance request from said requesting computer to an assessment computer responsible for assessment of whether said computer file contains malware (See Hruska Col. 3 Lines 20-24 and Col. 4 Lines 20-23);

file access clearance request receiving logic operable to receive at said assessment computer said file access clearance request from a requesting computer (See Hruska Col. 5 Lines 60-66); file access clearance response generating logic operable in dependence upon said data identifying said computer file to determine if said computer file has previously been assessed as not containing malware and to generate a file access clearance response (See Hruska Col. 5 Lines 3-10); file access clearance response transmitting logic operable to transmit said file access clearance response to said requesting computer (See Hruska Col. 5 Lines 66-67); file access clearance response receiving logic operable to receive at said requesting computer said file access clearance response from said assessment computer (See Hruska Col. 4 Lines 45-52 and Col. 5 Lines 66-67 wherein it was implied that the requesting workstation received the report because the file server sent the report to the workstation and the workstation used the report); and file access permitting logic operable if said file access clearance response indicates said computer file does not contain malware to permit said file access request by said requesting computer (See Hruska Col. 4 Lines 45-52), and wherein said assessment computer stares a database of computer files including for each file a checksum of the file when last determined to be valid (See Hruska Col. 5 Lines 14-18 and 22-25), but Hruska failed to disclose wherein said database includes for each computer file a persistence flag indicating whether an entry relating to said computer file should be purged from said database during purge operations.

Le Pennec teaches that in a virus detection system, in order to improve virus detection, a virus-free certificate should be associated with a file and stored in a database (See Le Pennec Col. 5 Lines 29-34 and Fig. 5 and associated text) as well as teaching that each certificate should have a hit count (511) which is used to determine if the certificate will be removed from the

database upon adding a new certificate to a "full" database (See Le Pennec Fig. 7 and associated text).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Le Pennec in the virus detection system of Hruska by utilizing the virus-free certificates in place of the checksums of Hruska. This would have been obvious because the ordinary person skilled in the art would have been motivated to improve upon the virus detection of Hruska.

Regarding claims 8, and 18, Hruska and Le Pennec disclosed that said data identifying said computer file includes a checksum value calculated from said computer file (See Hruska Col. 3 Lines 1-3 and Col. 4 Lines 13-16 and Le Pennec Fig. 5).

Regarding claims 9, and 19, Hruska and Le Pennec disclosed that said data identifying said computer file includes one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file (See Hruska Col. 5 Lines 43-48, and 51-56 and Le Pennec Fig. 5).

Regarding claims 10, and 20, Hruska and Le Pennec disclosed that if said file access clearance response indicates a scan of said computer file is required by said assessment computer, then computer file transmitting logic is operable to transmit said computer file from said requesting computer to said assessment computer, receiving at said assessment computer said computer file from said requesting computer and performing a malware scan of said computer file (See Hruska Col. 4 Lines 20-23 and 26-40 and Col. 5 lines 10-13).

Regarding claims 11 and 21, Hruska and Le Pennec disclosed that if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said assessment computer (See Hruska Col. 5 Lines 18-22).

Regarding claim 22, Hruska and Le Pennec disclosed that if said file access clearance response indicates access to said computer file is denied, then triggering a denied access response in said requesting computer (See Hruska Col. 4 Lines 52-55).

Regarding claims 12 and 23, Hruska and Le Pennec disclosed that said assessment computer stores a database of computer files previously assessed as to whether they contain malware (See Hruska Col. 5 Lines 14-18).

Regarding claims 13 and 24, Hruska and Le Pennec disclosed that said database includes for each computer file fields specifying one or more of a filename of said computer file, data identifying said requesting computer and a storage location of said computer file, a checksum value calculated from said computer file, an access flag indicating whether access to said computer file is denied and a persistence flag indicating whether entries relating to said computer file should be purged from said database during purge operations (See Hruska Col. 5 Lines 14-18 and 22-25 and Le Pennec Fig. 5).

Regarding claims 16, and 27, Hruska and Le Pennec disclosed that a plurality of requesting computers share access to an assessment computer for determining whether file access requests by those requesting computers should be denied (See Col. 5 Lines 26-40).

Claims 34-40, 43-51, and 54 are rejected for the same reasons as claims 7-13, 16-24, and 27 respectively, and further because Hruska disclosed the method of the above rejected claims (See Hruska Abstract).

Claims 61-67, 70-78, and 81 are rejected for the same reasons as claims 7-13, 16-24, and 27 respectively, and further because Hruska disclosed the system of the above rejected claims (See Hruska Abstract).

Claims 14-15, 24-25, 41-42, 52-53, 68-69, and 79-80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hruska and Le Pennec as applied to claims 7, 17, 34, 44, 61, and 71 above respectively, and further in view of Caccavale (US Patent Application Publication Number 2002/0129277).

Hruska and Le Pennec disclosed denying access to files in the event that they contain characteristic forms of viruses (See Col. 1 Lines 62-65 and Col. 4 Lines 45-55), but failed to disclose a message being sent to the file server indicating a switch to a mode of operation wherein more files are denied for access. Hruska does, however, disclose that a user can indicate that all files need to be checked by the file server regardless of prior results (See Hruska Col. 4 Lines 55-57).

Caccavale teaches that it is often the case that a virus checker program is unable to detect a new virus (See Caccavale Paragraph 0075 Lines 1-2). Caccavale further teaches that in such a case, an updated anti-virus pattern file should be distributed to the virus checker program, at which point all the files can be marked as unchecked in order for all the files to be checked for the new virus using the new pattern (See Hruska Paragraph 0075).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Caccavale in the file checking system of Hruska and Le Pennec by sending new anti-virus patterns to the file server, and in response to receiving the new

pattern, marking all the files as unchecked and needing to be scanned. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the workstations from files containing new viruses that the file server did not know of when the file was originally scanned. In this manner, the fileserver would rescan all the files with a greater likelihood of finding a virus and therefore denying access to more files.

Conclusion

Claims 7-27, 34-54, and 61-81 have been rejected.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Matthew Henning
Assistant Examiner
Art Unit 2131
7/26/2006